UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/734,102	12/11/2000	Rosario Gennaro	YOR920000597US1(13879)	3899

7590 12/06/2005

RICHARD L. CATANIA, ESQ.
SCULLY, SCOTT, MURPHY AND PRESSER
400 Garden City Plaza
Garden City, NY 11530

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/734,102	**Applicant(s)** GENNARO ET AL.	
	Examiner Aravind K. Moorthy	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 September 2005.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-5,7-9,11-13,15 and 16 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-5,7-9,11-13,15 and 16 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 28 March 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 23 September 2005.

2. Claims 1-5, 7-9, 11-13, 15 and 16 are pending in the application.

3. Claims 1-5, 7-9, 11-13, 15 and 16 have been rejected.

4. Claims 6, 10 and 14 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-5, 7-9, 11-13, 15 and 16 have been considered but are moot in view of the new ground(s) of rejection.

6. With the respect to the 112 first paragraph rejection, the examiner maintains the rejection. After further review of the specification, the examiner has found support for "an encrypted copy of the signed coin" but there is no support for an encrypted copy of the unsigned coin.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-5, 7-9, 11-13, 15 and 16 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The limitation "both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin" is not enabled by the specification. For the sake of examining, the examiner assumes that

if an entity is able to send back to the user a encrypted signed copy of the coin, then it is able to send back an unsigned copy.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 2, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Dent U.S. Patent No. 6,311,171 B1 in view of Oishi U.S. Patent No. 6,298,153 B1.

As to claim 1, Dent discloses a method of providing anonymous digital cash, the method comprising:

providing an entity with a secure co-processor [column 4, lines 39-65];

a user establishing a secure channel to a program running on the coprocessor [column 16, lines 18-30];

the user sending a coin to be digitally signed to the coprocessor using any secure digital signature algorithm [column 3, lines 54-58];

forming an encrypted copy of the signed coin and an encrypted copy of the unsigned coin using a public key of a given encryption scheme having the public key and a private key [column 4, lines 39-65];

Dent does not teach that signing the coin with a non-homomorphic signature and sending back to the user both the encrypted copy of the signed coin and the encrypted copy of the unsigned coin, the user having the private key of the encryption scheme, wherein the user is able to use the private key to decrypt both the signed and unsigned copies of the coin to use the coin as digital cash while keeping the identity of the user unknown to the coprocessor. Dent does not teach that the non-homomorphic signature scheme includes a private and public key. Dent does not teach that the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the unit.

Oishi teaches signing with a non-homomorphic signature and sending back to the user both an encrypted copy of the signed coin and an encrypted copy of the unsigned coin to enable the user to keep the identity of the user unknown to the coprocessor [column 11, lines 48-54]. Oishi teaches that the non-homomorphic signature scheme includes a private and public key [column 18, lines 44-53]. Oishi teaches that the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the unit [column 18, lines 44-53].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dent so that the coin would have been signed with a non-homomorphic signature to enable the user to use the coin while keeping the identity of the user unknown to the coprocessor. The non-homomorphic signature scheme would have included a private and public key. The step of using the non-homomorphic signature scheme would have included the step of using the private key of the non-homomorphic signature scheme to sign the unit.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dent by the teaching of Oishi because it provides anonymity of the user and safety of privacy protection can be further improved [column 18, lines 44-53].

As to claims 2, Dent teaches a method comprising the steps of:

the processor providing a signature to authenticate [column 3, lines 54-58];

the user using the coin for payment to a merchant [column 4 line 66 to column 5 line 43];

and the merchant returning the signed coin to the entity for credit to an account of the merchant [column 4 line 66 to column 5 line 43].

As to claim 15, Dent teaches a method, wherein:

the communicating step includes the step of the customer sending to the generator the public key of the encryption scheme [column 6 line 46 to column 7 line 32]; and

the step of using the secure cryptography generator includes the step of using the public key to encrypt the signature on the unit [column 6 line 46 to column 7 line 32].

9. Claims 3-5, 7-9 and 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Kravitz et al U.S. Patent No. 5,832,089.

As to claims 3, 7 and 11, Kravitz et al discloses a method of creating and managing electronic cash, comprising the steps:

a customer communicating to a secure cryptography generator a given encryption scheme having a public key and a private key, and a cash amount [column 8, lines 1-24];

establishing a unit representing the cash amount [column 7, lines 34-51];

signing the unit [column 8, lines 1-24];

using the secure cryptography generator to encrypt both the signed unit and the unsigned unit using the public key of the encryption scheme [column 15, lines 49-65];

storing in a database the encrypted signed unit and a value for the unit [column 15, lines 49-65];

transmitting back to the customer both the encrypted copy of the signed unit and the encrypted copy of the unsigned unit [column 15, lines 49-65];

the customer using the private key of the encryption scheme to decrypt both the encrypted signed unit and the encrypted unsigned unit to obtain the signed unit and the unsigned unit [column 15, lines 49-65]; and

using the signed unit as a payment [column 15, lines 49-65].

Kravitz et al does not teach signing the unit with a non-homomorphic signature to enable the customer to use the electronic cash while keeping the identity of the customer unknown to the coprocessor.

Oishi teaches signing with a non-homomorphic signature to enable the user to keep the identity of the user unknown to the coprocessor [column 11, lines 48-54]. Oishi teaches that the non-homomorphic signature scheme includes a private and public key [column 18, lines 44-53]. Oishi teaches that the step of using the non-homomorphic signature scheme includes the step of using the private key of the non-homomorphic signature scheme to sign the unit [column 18, lines 44-53].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kravitz et al so that the unit would have been signed with a non-homomorphic signature to enable the user to use the coin while keeping the identity of the customer unknown to the coprocessor.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Kravitz et al by the teaching of Oishi because it provides anonymity of the user and safety of privacy protection can be further improved [column 18, lines 44-53].

As to claims 4, 8 and 12, Kravitz et al teaches establishing an expiration date for the unit. Kravitz et al discloses storing the expiration date in the database [column 14 line 65 to column 15 line 10].

As to claims 5, 9 and 13, Kravitz et al teaches that the signing step includes the step of using the secure cryptography generator to sign the unit [column 8, lines 1-24].

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
November 29, 2005

Primary Examiner
AU 2131
11\30\05